FI Supervision

In-depth analysis of banks' systems for sanctions screening

No. 30
06 November 2024

FI Ref. 24-28848

Contents

Summary

Finansinspektionen's (FI) in-depth analysis into sanctions screening shows that the effectiveness of the automated systems that banks use for their sanctions screening could be higher in general and that there is room for some banks to improve their work in this area. However, FI makes the assessment that the banks in the sample in general have a good understanding of the sanctions regulations and suitable technical systems for complying with the regulations.

The scope of international sanctions has increased significantly in recent years. This is primarily due to Russia's full-scale invasion of Ukraine in February 2022. The aim of sanctions is to limit in various ways the actions of the sanctioned party. It is important for banks and other financial firms to take measures that enable them to comply with the sanctions and thereby achieve the desired impact. The large number of customers and transactions in the banking sector often means that suitable technical tools and automated systems for sanctions screening are a necessity.

Compliance with international sanctions is a prioritised area of supervision for FI in 2024, and this in-depth analysis of banks' systems for sanctions screening is a result of this focus. We conducted the analysis by testing the automated systems used in sanctions screening at 19 banks active in Sweden. The technical part of the test was conducted in the systems' test environment to measure how the systems performed against the sanctions lists from the UN and the EU. This means that the review of the systems' effectiveness and efficiency was based on the parameters and settings that each bank has in its system without including *actual* business relationships or transactions.

The tests show that none of the banks achieve 100 per cent effectiveness in the automated controls. In general, the effectiveness reflects the size of the bank and is higher the larger the bank. This could mean that risks are concentrated among small and mid-size banks. The analysis also shows that the effectiveness of transaction screening tends to be higher than the effectiveness of customer screening. The banks' sanctions screening also has significantly lower effectiveness for manipulated names than for the spelling of names precisely as they appear in the lists, particularly for customer screening. The banks with the lowest effectiveness in customer screening use the same automated screening system. There are also differences between banks that use the same system. This indicates that part of the effectiveness can originate in the banks' own management of the systems.

FI may follow up in its ongoing supervision or as part of investigations on the banks' compliance with the sanctions regulations.

Finansinspektionen's supervision

FI supervises the financial sector and is one of several authorities responsible for implementing international sanctions. FI performs tasks related to individual provisions in the EU's sanction regulations in its role as a national competent authority, makes decisions on interim freezing of funds in certain situations, and exercises supervision in the area. Its supervision assignment also includes monitoring financial firms' compliance with UN and EU sanctions.

Regulations on sanctions

The sanctions that apply in Sweden are decided by the UN Security Council and the Council of the European Union. The UN decides on sanctions by adopting resolutions that are binding for all Member States. UN resolutions and the EU's own restrictive measures that include targeted financial sanctions are implemented in regulations that are adopted by the Council of the European Union. These Council regulations are directly applicable in Swedish national law (hereafter referred to as *sanctions regulations*).

A sanctions regulation contains provisions on, for example, an obligation to freeze funds and economic resources owned or controlled by natural or legal persons specified in annexes to the sanctions regulations, so-called sanctions lists. The regulations also contain prohibitions on making funds and economic resources available to sanctioned parties.

FI makes interim freezing decisions

Since 1 January 2024, FI has been tasked with making interim freezing decisions pursuant to section 5a of the Certain International Sanctions Act (1996:95). The aim is to enact UN decisions on sanctions more rapidly than what is possible within EU decision processes. Such decisions must be made when the UN has listed a natural or legal person in a sanction regime that includes targeted financial sanctions without the EU having issued a corresponding decision. FI's decision applies until the EU has implemented a corresponding decision in a relevant sanctions regulation.

The sanctions regulatory framework is to be applied by all legal persons that in full or in part conduct business in the EU and by all EU citizens. The framework also applies to all operations in all situations, whether they refer to domestic transactions, cross-border transactions or customers in third countries.

FI supervises that banks comply with the rules that apply to their business (Chapter 13, section 2 of the Banking and Financing Business Act). In general, this supervision assignment includes reviewing that firms are able to comply with the

sanctions provisions. Individual breaches of sanctions are investigated law enforcement authorities.

Importance of financial firms following sanctions

In recent years, the use and scope of international sanctions have increased significantly. The primary reason for this increase is Russia's full-scale invasion of Ukraine in February 2022. There are currently in Sweden both sanctioned parties and assets belonging to sanctioned parties. There are Russian-owned firms and assets in Sweden as well.[1] The risk of breaches and circumvention of the sanctions regulatory framework has thereby increased.

The overarching purpose of the sanctions is to limit the actions of the sanctioned parties. In order for the sanctions to have the desired impact, it is necessary for banks and other financial firms to take measures to ensure compliance with the sanctions and prevent economic assets from being made available to sanctioned parties and freezing any assets owned or controlled by these parties.

The business conducted by banks in Sweden encompasses a large number of customers and transactions. If the banks are to be able to comply with the sanctions in practice, they will often need suitable technical tools and automated systems for sanctions screening. It is thus important for the banks to have a good understanding of both the regulatory framework and how the technical systems function. Given the rapid development in the area of sanctions, FI has identified sanctions compliance as one of its prioritised areas for supervision.

---

[1] See, for example, FOI (2022), *Ryska investeringar och ekonomiska intressen i Sverige*, and the Swedish Security Service's status report for 2023–2024.

The in-depth analysis

Implementation

In 2024, FI conducted an in-depth analysis (*thematic review)* into sanctions screening. For the analysis, we selected 19 banks that are active in Sweden. We then tested the automated systems these banks use for sanctions screening. The banks were chosen based on their size and business orientation in order to provide as broad and representative sample of the Swedish banking sector as possible. To conduct the tests, we engaged an external firm that provided technical assistance.

All the banks in the in-depth analysis use screening systems that are provided by external suppliers and then integrated with the banks' customer systems. The screening tools are used to review the banks' customers and transactions in order to identify any sanctioned parties, thereby ensuring compliance with the sanctions regulatory framework.

We conducted the tests in a so-called test environment to achieve a comparable understanding of the functionality in the systems that the banks use. This means that our review of the systems' effectiveness and efficiency was based on the parameters and settings that each bank had in its system. In other words, the analysis was conducted without reviewing actual customers or transactions. The review also did not include other measures and systems that the banks use to comply with the sanctions regulations. Even if the banks' tools for sanctions screening are of great importance for their ability to comply with the sanctions, the analysis does not draw any conclusions about actual deficiencies in or breaches of the sanctions regulatory framework.

Testing of automated screening systems

Through the tests, FI reviewed how the banks' automated screening systems – in a test environment – generated hits of both customers and transactions against the UN's and the EU's sanctions lists. Each bank was given a test list of 5,000 names from the UN's and the EU's sanctions lists to run against their systems.

The results show the systems' *effectiveness*, i.e., the percentage of the 5,000 sanctioned parties in the test file that the bank's systems successfully identified, for both customers and transactions. Through the tests we looked in particular at how well the systems could identify identification information such as the name and birth date of sanctioned parties as written in the lists and how well the systems identified this information after it had been manipulated and altered.

The effectiveness of the systems in identifying manipulated or altered names is of importance because there can be natural source errors in how names are spelled in

other written languages and alphabets. Compound names can be written in different ways, for example with or without a hyphen, accent, or apostrophe or written as one or several words. Using different spellings and variations of a name can also be one way to circumvent the sanctions.

In addition to effectiveness, FI also reviewed the *efficiency* of the banks' systems by measuring both the total number of alerts generated for each hit from the sanctions lists and the percentage of false alerts. Banks need to review all alerts generated by the systems in order to determine if it is a true hit, i.e. if the hit is actually on a sanctioned party. This review needs to be done promptly, which in turn requires resources. It is therefore in every bank's interest to reduce the number of excessive and false alerts generated.

In addition to testing the customer and transaction screening, we also conducted two *control tests*. The first control test measured whether the banks' systems generated hits for entities that are not included on any of the sanctions lists. For this test, a list of 200 non-sanctioned individuals and firms were test-run against the banks' systems. In the second control test, we reviewed whether the banks could identify a small number of sanctioned banks by testing if the systems reacted to their unique identifier code, BIC (Business Identifier Code).[2] The aim of the control tests is to provide an indication of how many false alerts are generated and how the systems are calibrated to identify a number of sanctioned banks.

The results of the tests are presented based on the number of banks and the systems the banks use. The results are presented anonymously and rounded to one decimal point in written text. In this report, the results have been aggregated for both the UN's and the EU's sanctions lists and for both natural persons and legal persons, unless otherwise specified.

In order for the reader to understand how the results compare to actual market shares, the results are also broken down into FI's supervision categories[3] and the share of established business relationships. The total number of business relationships for the 19 banks in the sample amounted to 20.3 million and are broken down into each supervision category as shown in *Figure 1*.

---

[2] Every bank has a unique identifier, BIC, that is used to identify banks and financial institutions around the world.

[3] FI separates credit institutions into four supervision categories depending on their degree of systemic importance. Category 1 includes the largest institutions. Category 2 includes mid-sized institutions, of which some are classified as large pursuant to Article 4(1)(146) of Regulation (EU) No. 575/2013. Category 3 includes smaller institutions. Category 4 includes small and non-complex institutions. For this analysis, we have also chosen to include foreign bank branches based on their weighted points in the four categories.

For all 123 banks active in Sweden, the total number of established business relationships amounts to 40.9 million.[4]

Figure 1. Breakdown of business relationships per supervision category in the sample.

Business relationships	Category 1	Category 2	Category 3	Category 4	All categories
Number	11,936,500	4,446,700	876,000	3,044,800	20,304,000
Share (per cent)	59	22	4	15	100

There are no established national or international benchmark indices that show how effective or efficient the sanctions screening tools used by banks and other financial institutions are. However, to gain insight into how the Swedish banking sector compares to banks and financial institutions in an international context, the results can be compared to corresponding tests conducted by 75 banks and financial institutions in several other countries in April 2024. These banks and financial institutions conduct corresponding tests continuously as part of a subscription service offered by the technical supplier of these tests. Given the limited number of institutions, their geographic spread, and that the sample includes both banks and other types of financial institutions, it is not possible to make a direct comparison, and the underlying data thus does not lead to any solid conclusions in the matter. However, even with these limitations, FI considers the provision of this reference to be contextually relevant and includes it below as the global average. The diagram shows the global average as a dotted line and the sample average as a yellow line.

---

[4] The data is obtained from the annual periodic reporting on money laundering.

Results from the in-depth analysis

Customer screening

In the first part, FI tested the banks' customer screening systems. This test included 21 systems since some of the 19 banks in the sample use more than one automated system.

Effectiveness

The analysis shows that, in a test where the names were spelled as they appear in the lists, the banks' customer screening systems could identify on average 86.3 per cent; the median value was 99.3 per cent. None of the banks achieved an effectiveness of 100 per cent, but eleven banks had an effectiveness of between 99.31 and 99.96 per cent; see *Figure 2*. For natural persons, the average was 82.9 per cent, and for legal persons 98.4 per cent. The effectiveness for the UN's list was on average 78.0 per cent, and for the EU's list 87.8 per cent.

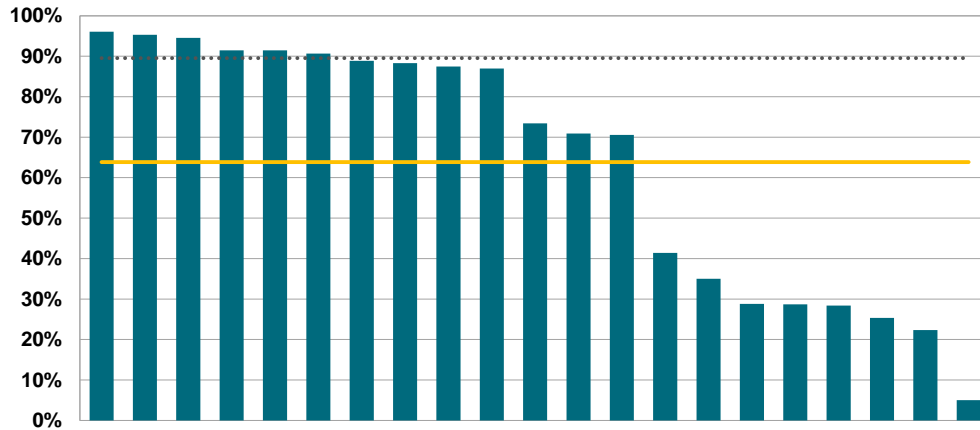Figure 2. Effectiveness for correctly spelled names in customer screening.
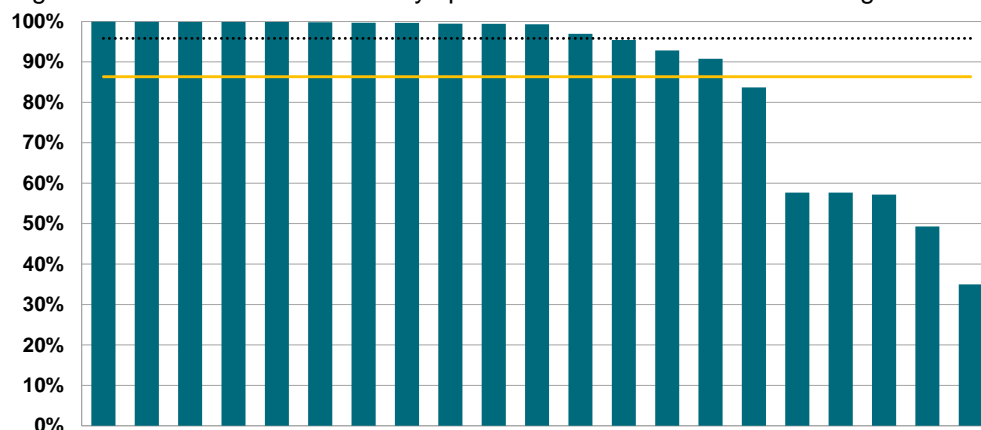
Note: The yellow line shows the sample average, and the dotted line shows a global average.

In a test where the spelling of the names had been manipulated, the banks' customer screening systems could identify on average 63.9 per cent, and the median was 73.4 per cent; see *Figure 3*. For natural persons, the average was 64.0 per cent, and for legal persons 63.5 per cent.

The results show that there is a large variation between the sample banks' systems; the highest effectiveness for manipulated names in the customer screening was 96.1 per cent while the lowest effectiveness was 5.0 per cent.

Figure 3. Effectiveness for manipulated names in customer screening.

Note: The yellow line shows the sample average, and the dotted line shows a global average.

A comparison of a test with correctly spelled names and a test with manipulated names shows that the effectiveness for manipulated names in banks' customer screening is on average 22.5 percentage points lower.

Four of the banks that have the lowest effectiveness for both correctly spelled names and manipulated names use the same system. The effectiveness for these banks in customer screening was on average 55.5 per cent for correctly spelled names and 27.8 per cent for manipulated names. The banks have noted that this could be due to their system required the names on the sanctions lists to be registered as customers in the system in order for it to be possible to conduct the test. The test data was not structured in the manner necessary to register all of the names listed in the test file as new customers; for example, the first and last name were not indicated. Given this, the banks take the position that the test results does not show a fair presentation.

Figure 4. Effectiveness in customer screening per supervision category.
Per cent
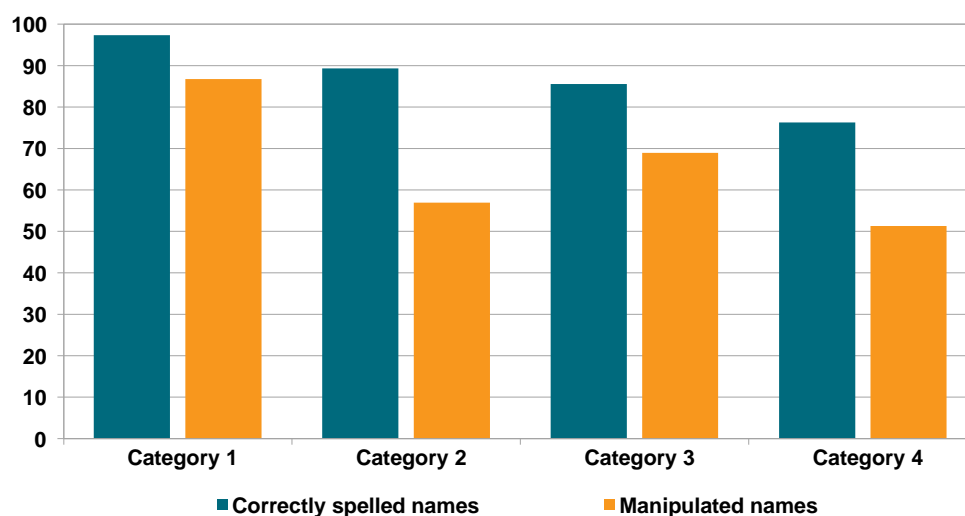
In order for the reader to understand how the results compare to actual market shares instead of the average per system, *Figure 4* shows the banks' customer screening effectiveness broken down into FI's supervision categories. This shows that the larger the bank, the higher the effectiveness, with some exceptions. If the customer screening effectiveness is broken down by the number of established business relationships, on average 91.9 per cent of the names on the sanctions lists were identified when correctly spelled and on average 74.2 per cent when the names were manipulated.

Efficiency

In the analysis, the efficiency in the banks' systems was measured using the number of alerts generated by the systems for every hit, with high efficiency meaning fewer alerts per hit. The banks' systems can generate one or more alerts for each positive hit for a name on a sanctions list. If the system's settings allow for the generation of multiple alerts, all of the alerts would need to be reviewed, which would require more resources from the bank. The total results for customer screening efficiency show that the banks in Category 4 have a higher percentage of alerts per hit than the other categories; see *Figure 5*.

Figure 5. Aggregate outcome for customer screening efficiency.

Number

Efficiency (number of alerts per hit)	Customer screening, correctly spelled names	Customer screening, manipulated names
Sample average	4.0	7.1
Sample median	4.0	4.1
Category 1 (average)	3.2	3.2
Category 2 (average)	3.5	4.1
Category 3 (average)	2.8	4.4
Category 4 (average)	5.5	13.4

The efficiency for correctly spelled names varies by the individual banks in the sample; *see Figure 6.*

Figure 6. Efficiency for correctly spelled names in customer screening.
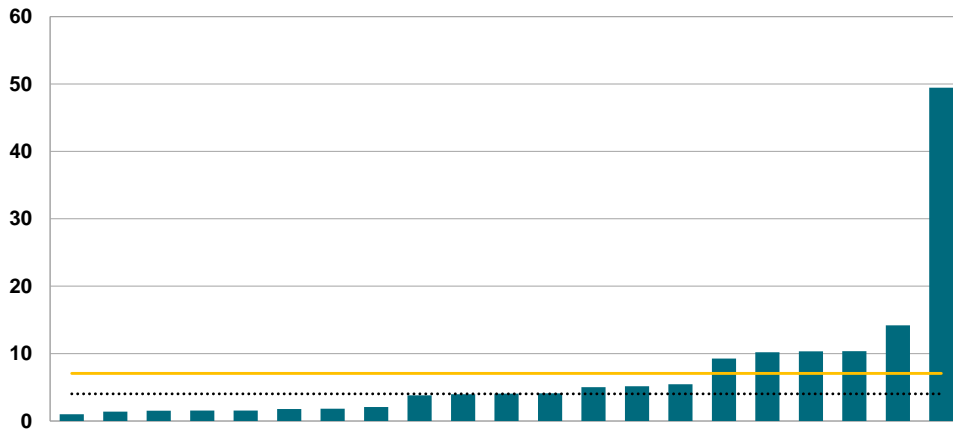
Average number of alerts per hit
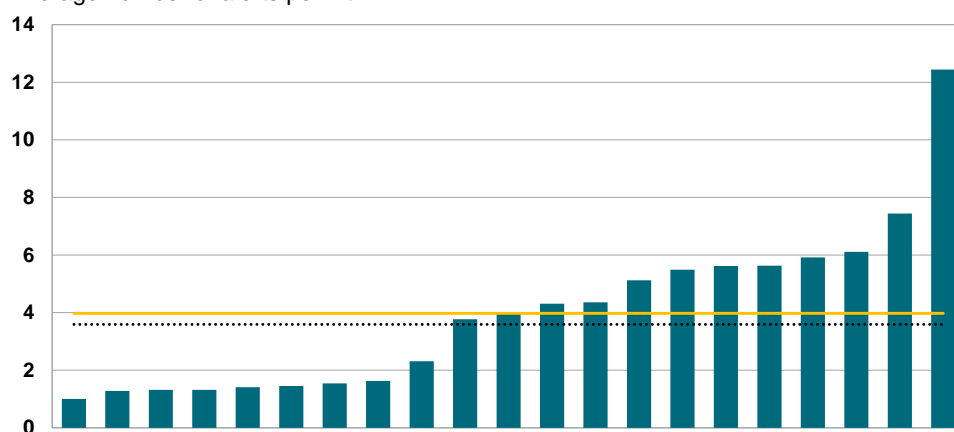
Note: The yellow line shows the sample average, and the dotted line shows a global average.

The results also vary greatly for manipulated names, with one of the systems deviating from the average with a high percentage of alerts. This means that the bank needs to investigate almost 50 alerts per hit; see *Figure 7.*

Figure 7. Efficiency for manipulated names in customer screening.
Average number of alerts per hit.

Note: The yellow line shows the sample average, and the dotted line shows a global average.

False alerts

Another way to assess efficiency in a system is to look at the number of false alerts. A high percentage of false alerts in relation to the total number of hits means lower efficiency since the banks need to allocate resources to investigate alerts that in reality can be disregarded. There is a considerable variation between the sample banks when it comes to false alerts. The ten banks with the largest share of false alerts in relation to the number of hits use the same four systems; see *Figure* 8.

Figure 8. Percentage of false alerts in relation to total number of hits.

Note: The yellow line shows the sample average.

Customer screening in an international context

The analysis shows that the banks in the sample had lower average effectiveness and efficiency in customer screening than the global average, which is evident from the results of corresponding tests for 75 banks and financial institutions. The effectiveness of the banks operating in Sweden for correctly spelled names was on average 86.3 per cent with an efficiency of 4.0, while the global average for effectiveness was 95.8 per cent with an efficiency of 3.6. The average for effectiveness for manipulated names for the banks operating in Sweden was 63.9 per cent with an efficiency of 7.1, while the global average for effectiveness was 89.5 per cent with an efficiency of 4.0.
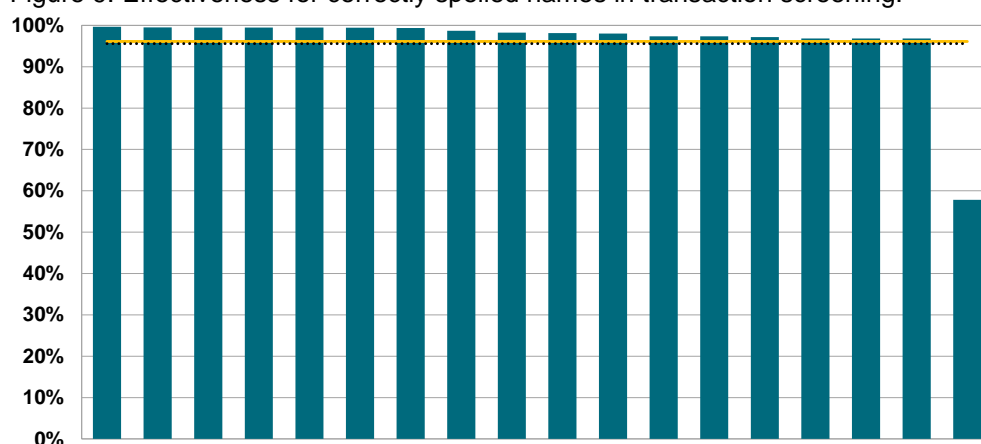
Transaction screening

In the second part, FI tested the banks' transaction screening systems. In total, 18 systems were tested since three banks in the sample use more than one automated system and four banks do not use any automated system.

Effectiveness

The analysis shows that the banks' transaction screening systems could identify on average 96.1 per cent of the names when spelled as they appear in the lists, and the median value was 98.2 per cent. None of the banks achieved an effectiveness of 100 per cent, but seven banks had an effectiveness above 99.3 per cent; see *Figure 9*. For natural persons, the average was 95.6 per cent, and for legal persons 98.1 per cent. The effectiveness for the UN's list was on average 91.5 per cent, and for the EU's list 96.9 per cent. One of the banks deviates from the average with a lower effectiveness of 57.8 per cent. When excluding the bank with the lowest transaction screening effectiveness, the average effectiveness was 98.4 per cent.
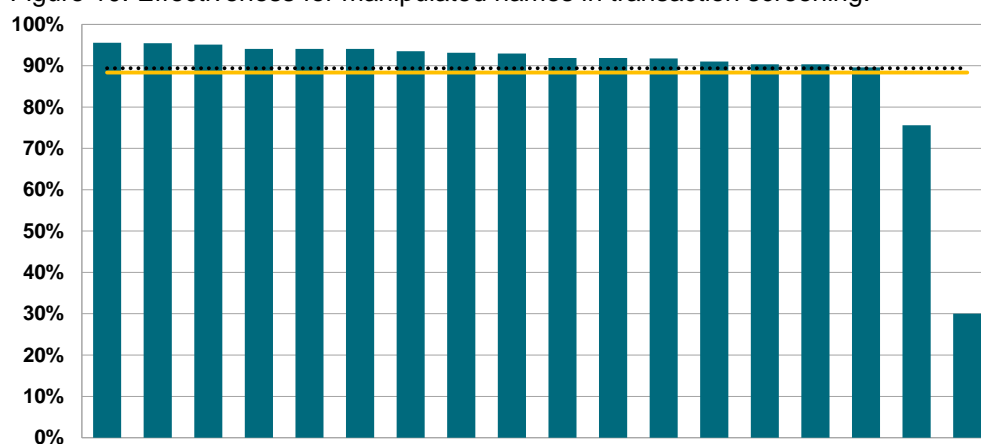
Figure 9. Effectiveness for correctly spelled names in transaction screening.

Note: The yellow line shows the sample average, and the dotted line shows a global average.

The banks' transaction screening systems could identify on average 88.4 per cent of the names on the sanctions list when manipulated, and the median was 92.4 per cent; see *Figure 10*. For natural persons, the average was 88.6 per cent, and for legal persons 87.5 per cent. When excluding the bank with the lowest transaction screening effectiveness for manipulated names, the effectiveness was on average 91.8 per cent.

Figure 10. Effectiveness for manipulated names in transaction screening.

Note: The yellow line shows the sample average, and the dotted line shows a global average.

The bank that had the lowest transaction screening effectiveness for correctly spelled names also had the lowest effectiveness for manipulated names, 30.0 per cent. Another bank deviates from the average with effectiveness of 75.6 per cent in a test with manipulated names. The same bank had an effectiveness of 99.5 per cent when screening for correctly spelled names.

A comparison of a test with correctly spelled names and a test with manipulated names shows that the banks' transaction screening effectiveness for manipulated names is on average 7.7 percentage points lower.

Figure 11. Effectiveness in transaction screening per supervision category
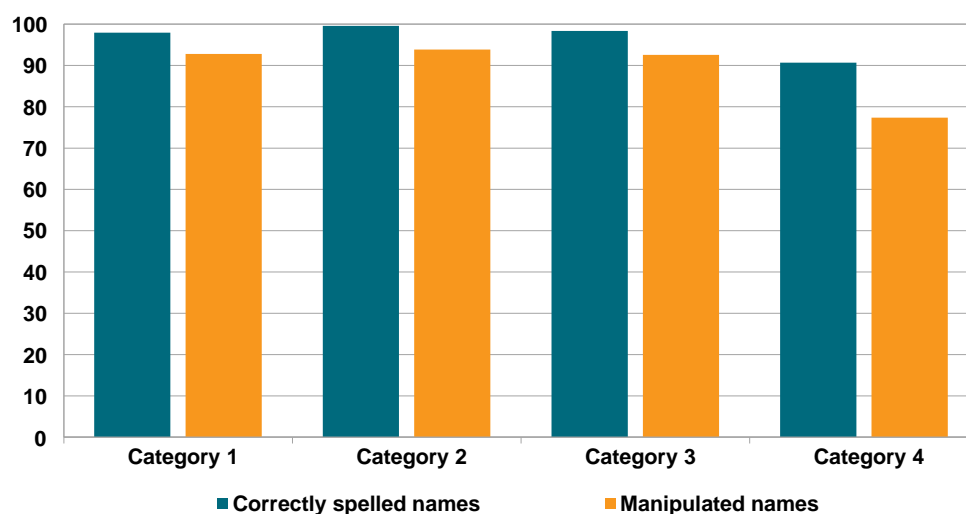Per cent

Figure 11 shows the banks' transaction screening effectiveness broken down into FI's supervision categories. This shows that the larger the bank, the higher the effectiveness, with some exceptions. If the effectiveness is broken down into the number of established business relationships, the percentage of correctly spelled names identified from the sanction lists is on average 97.2 per cent and manipulated names 90.6 per cent.

Efficiency

The total results for transaction screening efficiency are shown in *Figure 12*. The analysis shows that banks in Category 2 deviate from the others with a higher average number of alerts per hit.

Figure 12. Aggregate outcome for transaction screening efficiency.

Efficiency (number of alerts per hit)	Transaction screening, correctly spelled names	Transaction screening, manipulated names
Sample average	6.4	5.9
Sample median	6.3	5.7
Category 1 (average)	3.0	2.8
Category 2 (average)	10.2	9.4
Category 3 (average)	4.0	3.7
Category 4 (average)	8.5	7.6

The efficiency for correctly spelled names in transaction screening varies for each sample bank; see *Figure 13*.

Figure 13. Efficiency for correctly spelled names in transaction screening.
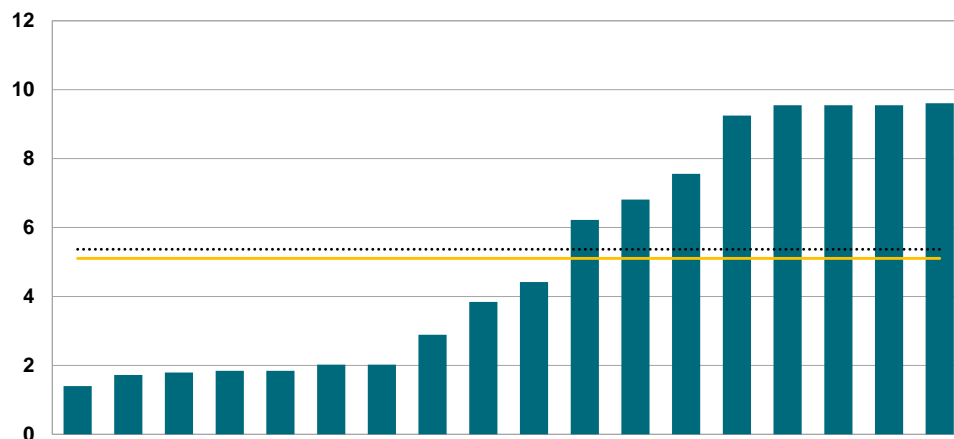Average number of alerts per hit
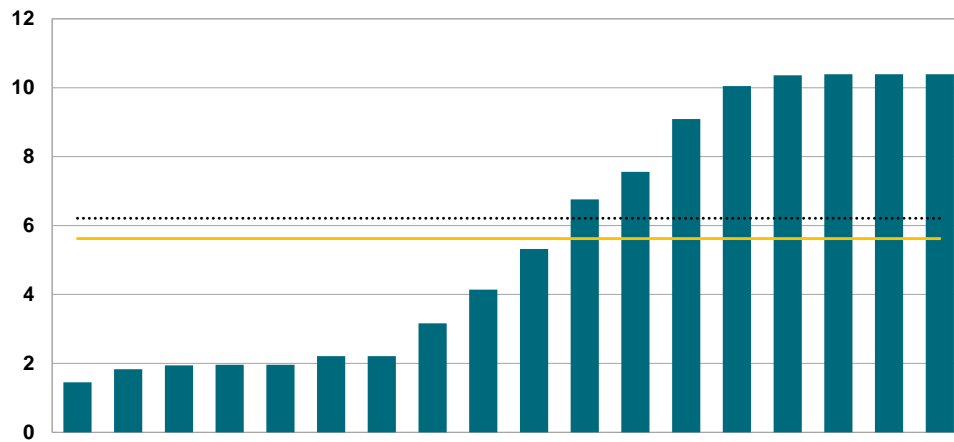
Note: The yellow line shows the sample average, and the dotted line shows a global average.

Just like for correctly spelled names, each bank's efficiency for manipulated names also varies; see *Figure 14*.

Figure 14. Efficiency for manipulated names in transaction screening.
Average number of alerts per hit

Note: The yellow line shows the sample average, and the dotted line shows a global average.

Four of the banks with the highest average number of alerts per hit and thus the lowest efficiency for both correctly spelled names and manipulated names use the same system.

False alerts

A comparison of the percentages of false alerts in relation to the number of hits shows differences between systems, with three systems deviating from the rest and the average for the sample of 9.3 per cent; see *Figure 15*. The bank that has a lower transaction screening effectiveness (57.8 per cent) also has a higher percentage of false alerts, 39.6 per cent. One of the banks that has the highest percentage of false alerts in its customer screening also has the highest percentage of false alerts in its transaction screening.

Figure 15. Percentage of false alerts in relation to the number of hits.
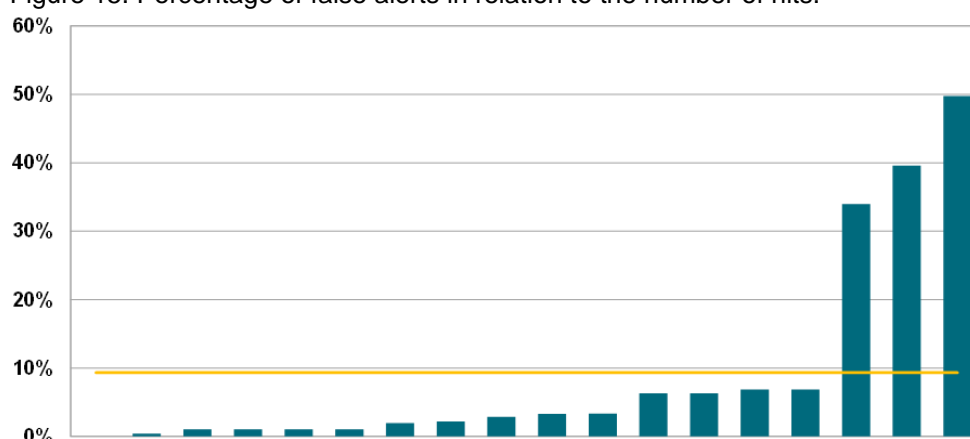
Note: The yellow line shows the sample average.

Transaction screening in an international context

With regard to transaction screening, the sample banks had marginally higher effectiveness and efficiency than the global average in the test with correctly spelled names. The average effectiveness for the banks operating in Sweden was 96.1 per cent with an efficiency of 5.6, while the global average for effectiveness was 95.6 per cent with an efficiency of 6.2. In the test with manipulated names, the sample banks had marginally lower effectiveness and higher efficiency than the global average. The average effectiveness for the banks operating in Sweden was 88.4 per cent with an efficiency of 5.1, while the global average for effectiveness was 89.4 per cent with an efficiency of 5.4.

Comparison between customer and transaction screening

The results for the effectiveness of the screening systems have been presented using the aggregate average for customer screening and transaction screening with correctly spelled names and manipulated names. The average result consists of the aggregate parameters *natural persons* and *legal persons* and *the UN's* and *the EU's*

sanctions lists. *Figure 16* shows the outcomes for these different parameters broken down to detail. We can see from the results some notable differences between the parameters, for example that effectiveness is higher for transactions than for customers, higher for legal persons than natural persons, and higher for the EU's list than the UN's list. Effectiveness is also higher when the results are broken down by the number of business relationships instead of per system.

Figure 16. Effectiveness broken down into certain parameters.

| Effectiveness	Customer screening, correctly spelled names	Customer screening, manipulated names	Transaction screening, correctly spelled names	Transaction screening, manipulated names
Aggregate (%)	86.3	63.9	96.1	88.4
Natural persons (%)	82.9	64.0	95.6	88.6
Legal persons (%)	98.4	63.5	98.1	87.5
UN sanctions list (%)	78.0		91.5	
EU sanctions list (%)	87.8		96.9	
Per number of business relationships (%)	91.9	74.2	97.2	90.6

Control tests

The analysis also included two control tests to review how the banks' screening systems reacted to non-sanctioned names and sanctioned banks' unique identifier codes (BIC).

Names not included on sanctions lists

A high percentage of false alerts means lower efficiency since the banks need to allocate resources to investigate alerts that in reality can be disregarded. The analysis shows that there is some variation among the results and that the banks' systems on average generated false alerts for 4.9 per cent of the cases in customer screening, i.e., alerts where the systems identified sanctioned parties that in reality were not sanctioned. One bank deviates with a high percentage of false alerts of 51.5 per cent non-sanctioned names. This is because the bank in question conducted the test using settings in its system that also generated hits against lists other than the UN's and the EU's sanctions lists; see *Figure 17*.
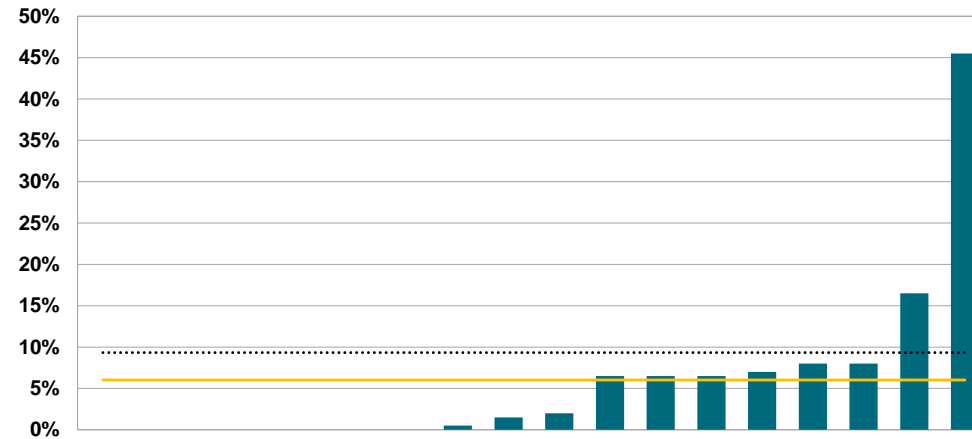
Figure 17. Percentage of false alerts for non-sanctioned names in customer screening.
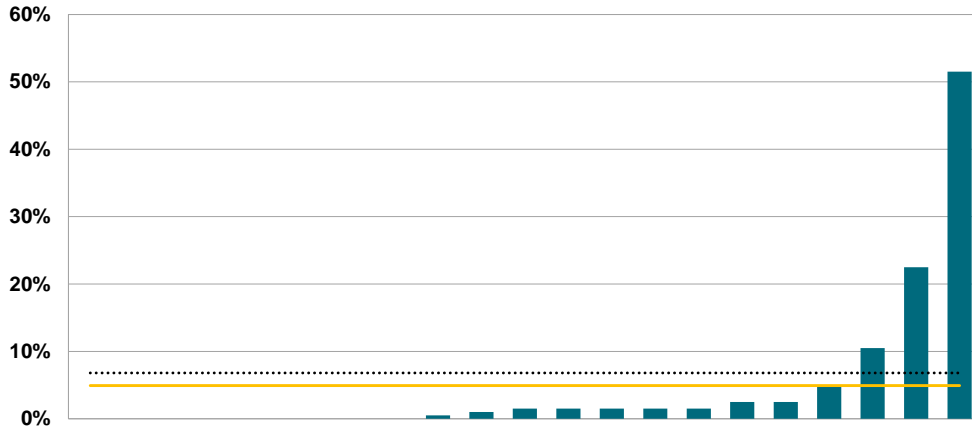
Note: The yellow line shows the sample average, and the dotted line shows a global average.

In the transaction screening, the average for false alerts was 6.0 per cent; see *Figure 18*. The results also vary here between banks, and the same bank deviates again with a high percentage of false alerts for non-sanctioned names for the same reason as above.

Figure 18. Percentage of false alerts for non-sanctioned names in transaction screening.

Note: The yellow line shows the sample average, and the dotted line shows a global average.
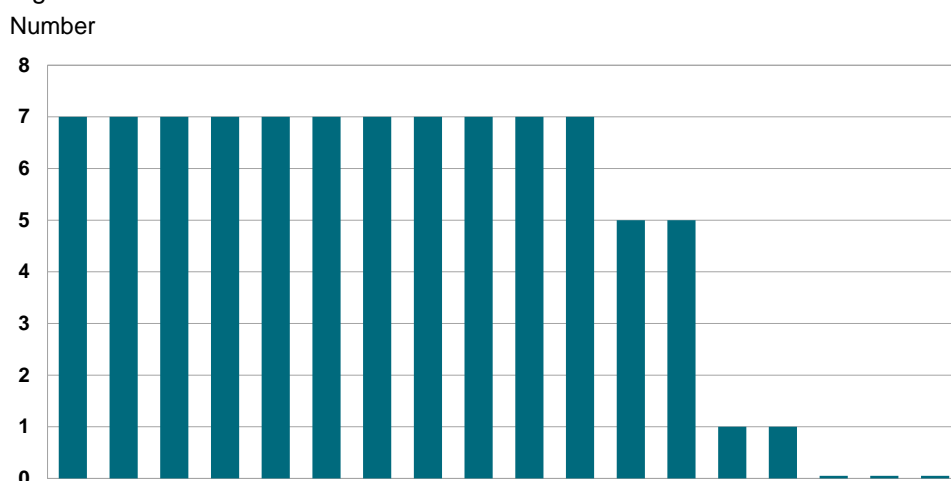
Sanctioned banks

Each bank has a unique identifier, BIC, that is used to identify banks and financial institutions around the world. In the test, FI reviewed whether banks' systems for

transaction screening identified seven sanctioned banks, the BIC codes of which are listed on sanctions lists. Five are North Korean, one is Libyan and one is Russian.

The analysis shows that the average hits for sanctioned BIC codes for all banks in the sample was 72.2 per cent (which corresponds to 5.1 BIC codes); see *Figure 19*. Three systems generated no hits for the seven sanctioned BIC codes, and two systems generated only one hit in transaction screening.

Figure 19. Effectiveness of sanctioned banks' BIC codes in transaction screening. Number

Control tests in an international context

With regard to false alerts for non-sanctioned names, the sample banks had a lower percentage of false alerts than the global average. In the customer screening, the average for the banks operating in Sweden was 4.9 per cent while the global average was 6.8 per cent. In the transaction screening, the average for the banks in the sample was 6.0 per cent while the global average was 9.3 per cent. For the test with sanctioned banks, there is no global average, and therefore no comparison.

Conclusions from the analysis

Based on the results of the analysis, FI sees that the effectiveness in the automated systems that the banks use in their sanctions screening in general could improve and that there is room for some banks to improve their work in this area. However, FI makes the assessment that the banks in general have a good understanding of and suitable technical systems for being able to comply with the sanctions regulations.

Effectiveness can improve

We can start by noting that none of the banks in the analysis have systems that successfully identified all names on the sanctions lists in the test environment. In their actual operations, we expect the banks to be able to comply with the regulations in full and identify all sanctioned parties. FI's message to the banks in the analysis is thus to take measures to improve the effectiveness and strengthen their ability to comply with the sanctions regulatory framework.

Effectiveness is largely correlated to the size of the bank; in other words, the larger the bank, the higher the effectiveness. In terms of the number of established business relationships and how they are distributed between the supervision categories, where almost 60 per cent of the total business relationships are found at Category 1 banks and almost 80 per cent at Category 1 and Category 2 banks, we see that effectiveness is higher for the majority of business relationships than for the sample. One conceivable explanation could be that larger firms often have more resources than smaller firms to allocate to compliance and adequate systems. One consequence of this could be that there is an elevated risk of transactions to and from sanctioned parties occurring through small and mid-size banks.

The screening systems' effectiveness against sanctions lists is most likely the result of not only the ability of the systems but also the banks' individual settings, threshold values, and established parameters for generating and eliminating alerts. Many of the systems use advanced algorithms, where seemingly small changes can have a comparatively large impact. These settings are often based on active decisions made by the banks and have a large impact on the systems' effectiveness. FI would like to emphasise that it is important for banks to test their systems regularly to understand how the systems work and perform in reality in order to achieve high effectiveness.

The analysis shows that the effectiveness in the banks' systems generally tends to be higher for transaction screening than customer screening. We find this somewhat surprising and draw the conclusion that some systems appear to have more difficulty identifying natural and legal persons that are both customers of the

bank and listed on the UN's or the EU's lists, than when these persons are the sender or recipient of a transaction or where the sanctioned party is included in the information accompanying the transaction.

The analysis also shows that some banks only use automated systems for transaction screening to a small extent or not at all. In some cases they use manual screening and in other cases they outsource the screening to other banks. We see that banks in the latter arrangement are not able to control or have any impact on the screening systems' functionality, settings and effectiveness. In turn this can lead to risks associated with third-party dependence.

We also note that some banks conveyed a perception that there is no legal obligation to screen domestic transactions. FI would like to highlight in this matter that there are both sanctioned parties and sanctioned assets in Sweden and that the sanctions regulatory framework does not make a distinction between domestic and cross-border transactions. It is thus every bank's obligation to ensure that it complies with relevant laws and regulations.

The analysis shows that banks' systems for sanctions screening in general have lower effectiveness for manipulated names than for correctly spelled names, particularly for customer screening. This means that the banks' systems in many cases require an exact match to generate a hit, and variations in spelling and the presentation of the name, birth date or other information could lead to the sanctioned parties not being identified by the systems. We would like to highlight that suitable technologies and measures, for example where algorithms identify variations of spellings and presentations of names, need to be in place and fine-tuned in order to be able to identify and achieve high effectiveness for manipulated names.

The analysis also shows that effectiveness is higher for the EU's sanctions list than for the UN's sanctions list for both customer and transaction screening. FI notes that, in order to achieve high effectiveness, banks' sanctions screening systems should be adapted to be able to capture changes in both the UN's and the EU's sanctions lists.

About some systems

It is important that the screening systems can identify and handle data that is structured in a way that agrees with the UN's and the EU's official sanctions lists in order to achieve high effectiveness. FI therefore takes the position that specific risks arise from using systems where the screening is limited due to the customer data being structured in the bank's customer systems in a way that differs with how the data is structured in the UN's and the EU's official sanctions lists.

Efficiency in the banks' systems varies

FI notes that efficiency in the banks' sanctions screening systems varies and that some systems have lower efficiency than others. Based on the strict requirements on compliance and that many banks are facing challenges from being able to manage thousands if not millions of customers and even more transactions, the efficiency of the systems is crucial for the amount of resources a bank needs to allocate to comply with the sanctions regulations. It should be in every bank's interest to continuously work to improve the efficiency of its systems.

Control tests

In the first control test, there were banks that generated alerts for a number of non-sanctioned names. A high percentage of false alerts means lower efficiency since the banks need to allocate resources to investigate alerts that in reality can be disregarded. Aside from one outlier, which can be explained by the bank's system settings when conducting the test, the average outcome shows a relatively low number of false alerts.

In the second control test with seven BIC codes, it can be noted that some sanctioned banks are not part of the international SWIFT system, which potentially reduces the risk of inadvertent payments to and from these banks. However, FI considers it to be important for banks to have procedures and controls in place in order not to risk the inadvertent occurrence of transactions to or from sanctioned parties.

Finansinspektionen's measures based on the analysis

FI expects banks and other financial institutions to comply with the legal requirements imposed upon them. This analysis is limited to reviewing the banks' automated sanctions screening systems and has not included other measures and systems that the banks could apply to comply with the sanctions regulatory framework. As presented in the analysis, there is room for several banks in the sample to improve their automated sanctions screening systems. In all cases, the banks have received individual feedback regarding the results from the analysis.

FI intends to use the results as part of its basis for risk-based supervision going forward. This means that we may follow up on individual undertakings in our ongoing supervision or through separate investigations.